COOLEY LLP
MATTHEW D. BROWN (196972)
(brownmd@cooley.com)
BETHANY C. LOBO (248109)
(blobo@cooley.com)
YUHAN ALICE CHI (324072)
(achi@cooley.com)
ERIK LAMPMANN-SHAVER (362460)
(elampmannshaver@cooley.com)
3 Embarcadero Center, 20th Floor
San Francisco, CA 94111-4004
Telephone: +1 415 693 2000
Facsimile: +1 415 693 2222

NAOMI HARRALSON MAY (291462)
(nmay@cooley.com)
NACHI A. BARU (345978)
(nbaru@cooley.com)
10265 Science Center Drive
San Diego, CA 92121-1117
Telephone: +1 858 550 6000
Facsimile: +1 858 550 6420

Attorneys for Defendant
RENAISSANCE LEARNING, INC.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION - SANTA ANA

M.C. 1 and M.C. 2, by and through their legal guardian NICOLE REISBERG, and M.C. 3 and M.C. 4, by and through their legal guardian AMY WARREN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

RENAISSANCE LEARNING, INC.,

Defendant.

Case No. 8:25-cv-01379-FWS-JDE

**DEFENDANT RENAISSANCE LEARNING, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT; MEMORANDUM OF POINTS & AUTHORITIES IN SUPPORT**

Date: February 5, 2026
Time: 10:00 a.m.
Courtroom: 10D

Pretrial Conference: March 9, 2028
Trial Date: April 4, 2028

TO PLAINTIFFS AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on February 5, 2026 at 10:00 a.m., in Courtroom 10D of the U.S. Courthouse located at 411 West 4th Street in Santa Ana, California 92701, Defendant Renaissance Learning, Inc. ("Renaissance") will and hereby does move the Court, pursuant to Federal Rule of Civil Procedure 12(b)(1) and 12(b)(6), to dismiss Plaintiffs' First Amended Complaint without leave to amend. For the reasons set forth in the accompanying Memorandum of Points and Authorities, Plaintiffs fail to state any claim upon which relief can be granted, requiring dismissal in full of their First Amended Complaint.

This motion is based upon this Notice, the accompanying Memorandum of Points and Authorities, the concurrently filed declaration of Bethany Lobo, the pleadings and papers on file in this action, and any further evidence or argument of counsel that the Court may receive at or before the hearing.

Dated: October 30, 2025

COOLEY LLP

By: */s/ Matthew D. Brown*
Matthew D. Brown

Attorneys for Defendant
RENAISSANCE LEARNING, INC.

# TABLE OF CONTENTS

**Page**

# TABLE OF AUTHORITIES

**Page(s)**

**Cases**

## TABLE OF AUTHORITIES
(continued)

**Page(s)**

## TABLE OF AUTHORITIES
(continued)

**Page(s)**

## TABLE OF AUTHORITIES
(continued)

**Page(s)**

## TABLE OF AUTHORITIES
(continued)

**Page(s)**



**Statutes**

## TABLE OF AUTHORITIES
(continued)

**Page(s)**



**Other Authorities**

## MEMORANDUM OF POINTS AND AUTHORITIES

## I. INTRODUCTION

Plaintiffs' First Amended Complaint ("FAC") again presents a lengthy, jumbled "think piece" reflecting their policy views on how the educational technology ("edtech") sector ***ought*** to function. The FAC does not, however, adequately state any of its claims. This is unsurprising: this case belongs to a series of ideologically driven lawsuits Plaintiffs' counsel have brought against major U.S. edtech providers, seeking to destroy a longstanding regulatory framework allowing schools to consent to edtech providers' collection of student data for educational use. The Court should reject this attempt to legislate through the courts.

All of Plaintiffs' claims are legally deficient. As before, Plaintiffs' wiretapping claims fail because they do not allege that Renaissance "intercepted" data in transit or aided third-party interception of such data. Nor do they plead that the data at issue constitutes "confidential communications" under Section 632 of the California Invasion of Privacy Act ("CIPA"), particularly as it is well-established that students in schools have a ***lesser*** legal expectation of privacy than the public. Plaintiffs' newly added CIPA Section 638.51 pen register claim fares no better, as Plaintiffs have not alleged an Article III injury. The claim also fails as a matter of law because it cannot apply to Renaissance's purported collection of IP addresses. Plaintiffs also fail to plead statutory standing—and fail to state a claim—under the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), California Unfair Competition Law ("UCL"), and Wisconsin Deceptive Trade Practices Act ("WDTPA"). Finally, Plaintiffs' new common-law claims under Wisconsin law fail. Plaintiffs cannot state an intrusion upon seclusion claim because they do not (and cannot) allege that Renaissance physically intruded into a "place." Their unjust enrichment claim fails because they do not adequately allege that Renaissance received a cognizable benefit from Plaintiffs. Nor can their novel negligence claim stand: their alleged harm (*i.e.*, Renaissance's alleged unlawful

collection and use of student data) was not "foreseeable" where Renaissance—like other edtech providers—has provided customary, valuable educational tools consistent with longstanding regulatory interpretations.

In sum, Plaintiffs' FAC repackages the deficient and conclusory allegations from the original complaint, demonstrating that further amendment would be futile and warranting dismissal with prejudice.

## II. FACTUAL BACKGROUND

### A. Renaissance Provides Valuable Tools to Aid Students' Learning

Renaissance contracts with schools and school districts to provide educational software and services. FAC ¶ 39. Schools and educators rely on Renaissance's tools to provide classroom instruction, administer student assessments, and analyze student learning. *See id*. Because these tools enhance the learning process, their use has become commonplace in students' lives. *See id*. ¶ 38 ("School districts access an average of nearly 3,000 EdTech tools during a school year. A single student accesses nearly fifty EdTech tools per year.").

Federal and state student data privacy laws recognize that schools need support from third-party service providers, including edtech companies, and thus contain exceptions to generally applicable consent requirements. Regulations implementing the federal Family Educational Rights and Privacy Act ("FERPA") and a similar California statute authorize schools to share student data with service providers for legitimate educational purposes—as determined by the school—without express parental consent. *See* 34 C.F.R. § 99.31(a)(1)(i)(A); Cal. Educ. Code § 49076(a). Both federal and California law also authorize service providers to disclose student data to third parties. *See*, *e.g.*, 34 C.F.R. § 99.33(b)(1) ("the party receiving the information may make further disclosures of the information" where doing so would, *inter alia*, further legitimate educational interests); Cal. Bus. & Prof. Code § 22584(b)(4) (allowing operator to "further disclose" information to, e.g., "allow or

improve operability and functionality").[1]

Renaissance's services comply with this well-established regulatory regime, which enables schools to utilize edtech vendors to enhance students' learning experience.

**B. Plaintiffs Allege Their Children Use Four Renaissance Products**

Plaintiffs Nicole Reisberg and Amy Warren bring this action on behalf of their minor children: (1) Reisberg's children, M.C. 1 and M.C. 2, who attended school in Orange County, California; and (2) Warren's children, M.C. 3 and M.C. 4, who attended school in Kansas. FAC ¶¶ 25–30. Plaintiffs allege that, collectively, their children used four of Renaissance's edtech products (the "Products"): (1) DnA, "a student-assessment and data-analytics platform" (*id*. ¶¶ 4, 77–80); (2) Fastbridge, an "assessment tool for monitoring and screening student progress" (*id*. ¶¶ 4, 61–65); (3) Nearpod, "an interactive instructional platform" (*id*. ¶¶ 4, 50–55); and (4) SAEBRS, a "screening tool used to [] identify students who may be at risk[.]" (*id*. ¶¶ 4, 68–74.)

Plaintiffs allege that the Products collect various student data. For example, they allege that DnA collected M.C. 1's and M.C. 2's names, student and school IDs, grade levels, attendance records, lunch balances, and guardian information. *Id*. ¶ 81. They allege that Nearpod collected M.C. 3's and M.C. 4's schoolwork, such as answers to multiple-choice questions. *Id*. ¶¶ 50–58. Fastbridge allegedly transmitted

[1] For more than two decades, the Federal Trade Commission ("FTC") has published guidance confirming that schools can consent on behalf of parents to the collection of personal information for educational purposes. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59903 (Nov. 3, 1999) (online operators can rely on school authorization); Complying with COPPA: Frequently Asked Questions, n. N, FTC, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%20SCHOOLS (last visited October 28, 2025) ("schools may act as the parent's agent and can consent under [the Children's Online Privacy Protection Act ('COPPA')] to the collection of kids' information on the parent's behalf").

information about M.C. 3's and M.C. 4's academic assessments to Renaissance. *See id.* ¶¶ 61–65. And M.C. 3 and M.C. 4 allegedly completed surveys ranking and describing their social and emotional well-being through SAEBRS. *Id.* ¶¶ 68–74.

In sum, Plaintiffs allege that Renaissance unlawfully collected, used, and shared their children's data via the Products, for commercial purposes and without directly obtaining their consent. *Id.* ¶¶ 5–10, 18–21.

## III. LEGAL STANDARD

### A. Rule 12(b)(1)

Federal Rule of Civil Procedure 12(b)(1) allows a defendant to move to dismiss a claim for lack of subject matter jurisdiction, including for lack of Article III standing. *Naruto v. Slater*, 888 F.3d 418, 425 n.7 (9th Cir. 2018). To bear their burden to establish Article III standing, plaintiffs must show "(1) a concrete and particularized injury, that (2) is fairly traceable to the challenged conduct, and (3) is likely to be redressed by a favorable decision." *Va. House of Delegates v. Bethune-Hill*, 587 U.S. 658, 662 (2019).

### B. Rule 12(b)(6)

To survive a Rule 12(b)(6) motion to dismiss, plaintiffs must allege "enough facts" to state a facially plausible claim to relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Factual allegations must create "more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Fraud-related factual allegations must satisfy Rule 9(b)'s heightened pleading requirements. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009). Plaintiffs must allege the "time, place, and specific content of the false representations" and "the parties to the misrepresentations." *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007) (citation omitted).

The court need not allow plaintiffs to amend where "any amendment would be an exercise in futility." *Steckman v. Hart Brewing, Inc.*, 143 F.3d 1293, 1298 (9th Cir. 1998).

## IV. ARGUMENT

### A. Plaintiffs' Federal and State Wiretapping Claims Fail Because They Have Not Alleged an "In Transit" Interception of "Content," Third-Party Involvement, or Recording of "Confidential" Communications (Counts I, II, and IX).

The federal Electronic Communications Privacy Act ("ECPA"), CIPA, and the Wisconsin Electronic Surveillance Control Law ("WESCL") prohibit the unauthorized interception of communications, and courts frequently analyze alleged violations of these statutes jointly. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (CIPA analysis "is the same as that under [ECPA]" (citation omitted)); *State v. Duchow*, 749 N.W.2d 913, 919 (Wis. 2008) (WESCL was intended to "effect the state 'implementation' of [ECPA]" and Wisconsin courts "employ[] reasoning from federal [wiretapping] decisions" when "interpreting the [WESCL]") (citation omitted)).

Plaintiffs baldly allege that Renaissance unlawfully intercepted the contents of their communications. *See* FAC ¶¶ 370, 375–376, 387, 490. But Plaintiffs fail to articulate a cognizable theory of "interception." On one hand, Plaintiffs allege that Renaissance is intercepting its own communications with them. *Id.* ¶ 178 ("These interactions are students' communications with Renaissance . . . . [and] these communications are intercepted by [Renaissance's product] Nearpod . . . simultaneously and in real-time when the student takes each of those actions on the product"). This theory fails because a recipient of a communication cannot legally intercept it. *See, e.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (ECPA and CIPA exempt parties to communications from liability); *Desnick v. Am. Broadcasting Companies, Inc.*, 44 F.3d 1345, 1353 (7th Cir. 1995) ("The federal and [Wisconsin] wiretapping statutes . . . allow one party to a conversation to record the conversation" unless the interception is done for a criminal or tortious purpose). On the other hand, Plaintiffs suggest that Renaissance intercepted their children's activities on ***third-party*** websites. *See* FAC ¶ 371

("communications intercepted by Renaissance included 'contents' of electronic communications made from Plaintiffs . . . to websites and other web properties ***other than*** Renaissance's"). But these allegations are speculative. Plaintiffs do not identify the alleged third-party websites or "web properties," let alone how Renaissance deployed its technology on these sites to intercept Plaintiffs' communications. In short, the Court should dismiss the wiretapping claims, whether they are based on allegations that Renaissance intercepted its own communications with Plaintiffs or eavesdropped on Plaintiffs' communications with unidentified third parties.

Plaintiffs' interception claims fail for additional reasons.

No "in transit" interception. For a communication to be "intercepted," it "must be acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). Courts routinely dismiss wiretapping claims where plaintiffs fail to allege facts showing that their communications were wiretapped in real time. *See Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751, 758 (N.D. Cal. 2023) (dismissing wiretapping claim alleging defendant's code "secretly intercept[ed] [communications] in real time" as "[t]hat statement does little more than restate the pleading requirement of real time interception"); *Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1019 (C.D. Cal. 2023) (similar).

Here, Plaintiffs attempt to satisfy this pleading requirement by making unsupported assertions that Renaissance's platforms ***can*** collect user information in "real time" without alleging facts showing that these interceptions took place (1) as described or (2) as to Plaintiffs' children, specifically. *See* FAC ¶¶ 147, 152, 156, 158, 162–64, 171, 178, 181, 187, 191, 196, 198, 202–04, 212, 220. Another court in this District dismissed near-identical wiretapping claims on this basis. *See Hernandez-Silva v. Instructure, Inc.*, No. 2:25-cv-02711-SB-MAA, 2025 WL 2233210, at *5 (C.D. Cal. Aug. 4, 2025) (dismissing CIPA claims where the

complaint "only vaguely references [d]efendant's use of [Application Program Interfaces or APIs] without explaining how the technology allows real-time interception in general or how it was used to intercept [p]laintiffs' data in particular").[2] This Court should likewise dismiss Plaintiffs' wiretapping claims.

No third-party involvement. Plaintiffs' CIPA Section 631 claim fails for additional reasons. They allege that Renaissance "aided and assisted numerous third parties . . . to unlawfully intercept protected communications[.]" FAC ¶ 391. This apparently attempts to allege a violation of clause four of CIPA Section 631(a), which imposes liability on someone "who aids, agrees with, employs, or conspires with any person or persons to" advance an act of eavesdropping or wiretapping.

Courts reject CIPA claims premised on third-party involvement where, as here, the third parties are service providers who passively store the data for a client's later retrieval or analysis (rather than independently using the data). *See Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 832 (N.D. Cal. 2021) (dismissing CIPA claim because service provider was not an eavesdropper, as it merely "provide[d] a software service that capture[d] its clients' data, host[ed] it on [provider]'s servers, and allow[ed] the clients to analyze their data"). Of the 17 third-party "vendors" Plaintiffs identify, FAC ¶ 136, they concede that many only provide passive technical functions such as "engineering support." To the extent they allege that any vendors assist with more "involved" functions such as "product development," Plaintiffs do not allege any facts showing that Renaissance provides these vendors student PII for these functions.[3] *See* FAC ¶ 132 (conclusory allegations that Renaissance "discloses personal information" to vendors). Plaintiffs do not plausibly allege that any vendors participated in any direct, simultaneous recording of communications on

[2] The *Instructure* plaintiffs did not assert ECPA or WESCL claims.

[3] Plaintiffs purport to cite to a Renaissance "product privacy policy," FAC ¶ 137 n. 19, to establish their allegations regarding third-party disclosures, but the link referenced in that footnote does not contain the disclosures that they claim.

Renaissance's platform.[4] *Cf. Q.J. v. PowerSchool Holdings LLC*, No. 23-5689, 2025 WL 2410472, at *1, 8 (N.D. Ill. Aug. 20, 2025) (denying dismissal of CIPA claim based on particularized allegations that a third-party provider "automatically capture[d] [] user interactions on [defendant's platform], from the moment of installation forward, including every click, swipe, tap, pageview, and fill" (internal quotations and citations omitted)). Plaintiffs do not allege facts—outside of their self-serving "description[s]" (*see* FAC ¶ 136)—that any of these vendors independently used Renaissance data, as would be required for an aiding and abetting claim. *See Graham*, 533 F. Supp. 3d at 832.

No "confidential communications." Section 632 applies only to "confidential communications," where one party "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002). "[I]n California, courts have developed a presumption that Internet communications do not reasonably give rise to that expectation." *Revitch v. New Moosejaw, LLC*, No. 18-CV-06827-VC, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019); *see also Boulton v. Community.com, Inc.*, No. 23-3145, 2025 WL 314813, at *2 (9th Cir. Jan. 28, 2025) (Section 632 does not apply to any text-based communications because they "are by nature recorded").

Plaintiffs' Section 632 claim is predicated on Renaissance's "non-consensual tracking of the Plaintiffs' and Class members' ***internet communications***[.]" FAC ¶ 387 (emphasis added). This is insufficient. Further, as discussed *supra*, Plaintiffs affirmatively allege that Renaissance publicly discloses as part of its privacy notice[5]

[4] This includes Mixpanel, for whom Plaintiffs again offer only cursory, unsupported allegations of real-time interception. *See* FAC ¶¶ 171–181.

[5] The privacy notice is incorporated by reference into the FAC, which repeatedly quotes it, and may be considered by the court in resolving this motion. *See* FAC ¶¶ 86, 99, 233, 250; *8 Lane Inv., Inc v. GenTech Sci., Inc.*, No. 822CV01686FWSKES, 2022 WL 20182971, at *2 n. 1 (C.D. Cal. Mar. 16, 2022)

that "dozens" of vendors may have access to personal information. *Id.* ¶¶ 136–137. Given Renaissance's public disclosure of the scope of potential data sharing, they had no "objectively reasonable expectation" that student communications would not be "overheard or recorded." *See Hubbard v. Google LLC*, No. 19-CV-07016-SVK, 2024 WL 3302066, at *7 n.9 (N.D. Cal. July 1, 2024) ("reasonable users should expect the collection of their internet-browsing data" particularly where complaint admitted awareness of "commonplace collection . . . of such data"). Indeed, Plaintiffs' awareness of Renaissance's data collection practices is illustrated by the FAC's allegations, which are based on publicly available sources. *See* FAC ¶¶ 108–151.

Finally, Plaintiffs' allegation that their children had "objectively reasonable expectations of privacy in their devices and activity," FAC ¶ 390, disregards long-established precedent that "students at school have a lesser expectation of privacy than members of the public generally." *Bravo ex rel. Ramirez v. Hsu*, 404 F. Supp. 2d 1195, 1201 (C.D. Cal. 2005) (citing *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 656-57 (1995)). The "devices" that students used to access Renaissance's educational services were also school property, further illustrating that students had no objectively reasonable expectation of privacy, particularly vis-à-vis the edtech provider and its vendors. FAC ¶¶ 25–29.

### B. Plaintiffs' CIPA Pen Register Claim Fails for Multiple, Independent Reasons (Count III).

Plaintiffs allege a CIPA pen register claim in the alternative to their CIPA wiretapping claim. CIPA prohibits installing a pen register device without a court order. Cal. Penal Code § 638.51(a). A "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is

(Slaughter, J.) (on a motion to dismiss, considering undisputedly authentic documents which were hyperlinked in the complaint).

transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

Plaintiffs theorize that Renaissance's products are pen register devices because they collect users' IP address.[6] This strains CIPA's plain text, which says nothing about IP addresses. Fundamentally, this is inconsistent with how the Internet works: all website operators receive visitors' IP addresses when loading the pages requested by those visitors.[7] This requires dismissal of Plaintiffs' pen register claim for two reasons.

***First***, Plaintiffs lack Article III standing to bring their CIPA pen register claim because they have suffered no injury in fact. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (plaintiffs must "have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) 'actual or imminent, not 'conjectural' or hypothetical[.]'") (citations omitted). Courts have repeatedly held that "there is no legally protected privacy interest in IP addresses." *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1189 (N.D. Cal. 2020) (dismissing CIPA claim for lack of Article III standing); *see also, e.g.*, *Khamooshi v. Politico LLC*, 786 F. Supp. 3d 1174, 1179–80 (N.D. Cal. 2025) (similar; collecting cases). Since Plaintiffs' pen register claim is based on the alleged collection of their IP addresses, in which they have no privacy interest, they have suffered no injury and

---

[6] Plaintiffs briefly reference "Device Metadata," which they contend also comprises "routing, addressing, or signaling information" collected by Renaissance's products. *See* FAC ¶ 399. However, they never explain the process through which this data is purportedly collected—nor do they clarify whether the process is the same for all Renaissance products. Indeed, the phrase "Device Metadata" is only ever referenced in conclusory allegations relating to Plaintiffs' pen register claim and occurs nowhere else in the FAC. *See id.* at ¶¶ 399, 401–03.

[7] *See, e.g.*, *What is an IP address?*, NORTON (last updated Apr. 15, 2025), https://us.norton.com/blog/privacy/what-is-an-ip-address ("Google and other web services know your IP address because it's assigned to your device and is required to connect to the internet in the first place."). This fact is judicially noticeable under Federal Rule of Evidence 201 as a fact generally known within this Court's jurisdiction.

lack standing.

The Ninth Circuit's recent opinion in *Popa v. Microsoft Corporation* illustrates as much. 153 F.4th 784 (9th Cir. 2025). There, the plaintiff alleged that Microsoft's session replay software—which monitored users' keystrokes while interacting with websites—violated state wiretapping and privacy tort law. The court held that the plaintiff did not "explain how the tracking of her interactions with the [ ] website caused her to experience any kind of harm that is remotely similar to the 'highly offensive' [privacy] interferences or disclosures that were actionable at common law[,]" and which could confer Article III standing. *Id.* at *5. This binding precedent applies: Plaintiffs do not (and cannot) allege a "highly offensive" privacy invasion that would have been actionable at common law based on the disclosure of their IP addresses to Renaissance. Thus, they have not adequately pled Article III standing. This Court lacks jurisdiction and should dismiss Plaintiffs' pen register claim on this basis alone.

***Second***, even if this Court had jurisdiction, it would fail because CIPA's pen register prohibition does not apply to IP address information. CIPA's pen register prohibition is a criminal statute. Cal. Penal Code § 638.51. As such, it should be applied "as favorably to the defendant as the language of the statute and the circumstances of its application may reasonably permit." *Walsh v. Dep't of Alcoholic Beverage Control*, 59 Cal. 2d 757, 764–65 (1963); *see also Jane Doe v. Eating Recovery Ctr., LLC*, No. 23-cv-05561-VC, 2025 WL 2971090, at *1 (N.D. Cal. Oct. 17, 2025) (urging courts to "resolve CIPA's many ambiguities" in favor of "narrower but equally reasonable interpretation[s]" which do not extend liability to new technologies not mentioned by the statute). This principle applies "even when," as here, "the underlying action is civil in nature." *Walsh*, 59 Cal. 2d at 765.

A court's "fundamental task in construing a statute is to ascertain the intent of the lawmakers so as to effectuate the purpose of the statute." *Day v. City of Fontana*, 25 Cal. 4th 268, 272 (2001). Here, the intent of California lawmakers—as

demonstrated by CIPA's statutory language and legislative history—shows the pen register prohibition does not apply to collection of IP addresses.

CIPA's legislative history shows that the Legislature was focused on "authoriz[ing] state and local law enforcement to seek emergency orders for pen registers/trap and trace devices used in telephone surveillance." Cal. Assem. Comm. on Privacy & Consumer Prot., Analysis of A.B. 929, 2015-2016 Leg., Reg. Sess. (Apr. 21, 2015). The Legislature has since updated CIPA multiple times "in response to the emergence of new communication devices," *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 191 (2021), but has never included IP address information.

Thus, neither the statutory definition of "pen register" nor the legislative history shows that the Legislature intended for CIPA's pen register provision to govern ***every*** instance of IP address collection. These collections occur innumerable times each second, every time a person visits a website as an inherent part of the process. *See Capitol Records Inc. v. Thomas-Rasset,* No. 06-1497 (MJD/RLE), 2009 WL 1664468, at *3 (D. Minn. June 11, 2009) ("standard computer operations require recording IP addresses so parties can communicate with one another over the Internet."). This is unsurprising. Interpreting the pen register prohibition to apply to the collection of IP address information would require website operators to collect consent before loading webpages, needlessly complicating web browsing.

As courts in California have recognized, nothing in the statute shows that the Legislature intended such a result. *See, e.g.*, *Licea v. Hickory Farms, LLC*, No. 23STCV26148, 2024 WL 1698147, at *4 (Cal. Super. Ct. L.A. Cnty. Mar. 13, 2024) (sustaining demurrer because "public policy strongly disputes" the notion that "every single [website] voluntarily visited by a potential plaintiff" has "violat[ed]" CIPA's pen register prohibition by collecting plaintiff's "IP address for purposes of connecting the website"); *see also* Order at 4, *Levings v. Open Text Corp.*, No. 24STCV05440 (Cal. Super. Ct. L.A. Cnty. Sept. 3, 2024) ("[T]he [operative complaint] is merely describing what happens every time a user accesses any

website."); Order at 3, *Rodriguez v. Plivo Inc.*, No. 24STCV08972 (Cal. Super. Ct. L.A. Cnty. Oct. 2, 2024) (similar); Order at 3, *Scharon v. Paramount Global*, No. 25STCV10585 (Cal. Super. Ct. L.A. Cnty. Oct. 3, 2025) (similar); Order at 5, *Sanchez v. Letter Four*, No. 24STCV18924 (Cal. Super. Ct. L.A. Cnty. Apr. 17, 2025) (similar). Courts examining the Federal Pen Register Act—upon which the California pen register statute was modeled—have reached similar conclusions. *See, e.g.*, *Capital Records Inc*., 2009 WL 1664468, at *3 (finding that an "IP address is transmitted as part of the normal process of connecting one computer to another over the Internet" and consequently, "the Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them. If it did apply in those cases, then the Internet could not function[.]"); *see also Malibu Media LLC v. Pontello*, No. 13-12197, 2013 WL 12180709, at *3–4 (E.D. Mich. Nov. 19, 2013) (the Pen Register Act does not prevent a third party from accessing a user's IP address because, by using the website, the user consensually engaged and "communicated his IP address").

Further, Plaintiffs' interpretation of the pen register statute is in tension with California's Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100 *et seq.* The CCPA created a balanced regulatory framework for data collection, processing, and sharing which reflects the California Legislature's current perspective on online privacy—unlike CIPA, which was enacted in 1967, well before the advent of the internet. *See Doe*, 2025 WL 2971090, at *3, *6 (expressing doubt that the California Legislature would have ever intended CIPA to encompass certain routine web browsing experiences where (i) "CIPA was enacted in 1967[,]" (ii) [i]ts language . . . is ill-suited for application to internet communications[,]" and (iii) "California has since adopted other statutes that more clearly speak to the practice of data sharing," like the CCPA). The CCPA framework also ***permits*** what Plaintiffs seek to prohibit. That is, the CCPA permits website operators to collect users' personal data, subject to procedural formalities, when that data is "reasonably necessary and

proportionate to achieve the purposes for which the personal information was collected or processed[.]" *Id.* § 1798.100(c). Collecting an IP address—a step that is necessary every time a webpage loads—is plainly "reasonably necessary." *See id*; *see also Capitol Records Inc.*, 2009 WL 1664468, at *3.

Plaintiffs' misinterpretation of CIPA's pen register provision would be untenable, as a California court explained this month: "If CIPA and the limitations on pen registers and trap and trace devices categorically prohibit collection of [IP address information] from website visitors, then the CCPA's provisions permitting reasonable collection of such data are a nullity. That would be an improper way to interpret and harmonize California law." *See* Order at 2–3, *Scharon v. Paramount Global*, No. 25STCV10585 (Cal. Super. Ct. L.A. Cnty. Oct. 3, 2025); *see generally Nat'l Indem. Co. v. Garamendi*, 233 Cal. App. 3d 392, 405 (1991) ("[C]ourts must construe a statute so as not to conflict with the other legislative enactments.").

Accordingly, Plaintiffs' CIPA pen register claim fails and should be dismissed without leave to amend.

### C. Plaintiffs Lack CDAFA Standing and Fail to Plead a CDAFA Violation (Count IV).

Plaintiffs' CDAFA claim repeats the same deficient allegations as before and fails for the same reasons.

CDAFA is an "anti-hacking statute" designed to "prohibit the unauthorized use of any computer system for improper or illegitimate purpose[s]." *Custom Package Supply, Inc. v. Phillips*, No.15:cv-04584-ODW-AGR, 2015 WL 8334793, at *3 (C.D. Cal. Dec. 7, 2015); Cal. Penal Code § 502(a) (statute meant to combat the "proliferation of computer crime[s]"). CDAFA exists to address data breaches, hacking, and other unauthorized access—a fundamental mismatch with Plaintiffs' theory. Unsurprisingly, then, Plaintiffs both lack statutory standing and have not otherwise stated this claim.

CDAFA standing requires a showing of "damage or loss." Cal. Penal Code

§ 502(e)(1). The "damage or loss" requires "some damage to the computer system, network, program, or data contained on that computer." *Heiting*, 709 F. Supp. at 1020–21; *Instructure*, 2025 WL 2233210, at *6. Plaintiffs only allege that Renaissance "was unjustly enriched by acquiring the valuable personal information of [Plaintiffs] . . . without permission and using it for Renaissance's own financial benefit to advance its business interests." FAC ¶ 412. This does not confer CDAFA standing.

To start, this allegation is conclusory: there are no factual allegations that Renaissance profited from, for example, selling the contested data to data brokers or using it to advertise. This theory of "damage or loss" is also fundamentally a privacy violation theory, which does not confer CDAFA standing. *See, e.g.*, *Doe v. Cnty. of Santa Clara*, No. 23-cv-04411-WHO, 2024 WL 3346257, at *9–10 (N.D. Cal. July 8, 2024) (no CDAFA standing where plaintiff alleged that "Defendants took something of value from Plaintiff . . . and derived benefit therefrom without Plaintiff's . . . knowledge or informed consent and without sharing the benefit"); *Heiting*, 709 F. Supp. 3d at 1020–21 (collecting cases holding that privacy violations based on loss of data "do not qualify [as 'damage or loss'] under the statute"); *Doe v. Tenet Healthcare Corp.*, 789 F. Supp. 3d 814, 845 (E.D. Cal. June 9, 2025) (finding no CDAFA standing where Plaintiffs alleged that "their medication information has economic value and that Defendants unjustly profited from" obtaining it).

Beyond standing deficiencies, Plaintiffs again fail to plausibly plead a CDAFA claim. They allege that Renaissance violated CDAFA section 502(c)(2) by "knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' and Class members' data." *Id.* ¶ 410. This does not suffice.

***First***, Plaintiffs' allegation that Renaissance acted "knowingly" "without permission" is contradicted by their admission that Renaissance "relie[d] on the consent of school personnel" to process students' data. *See id.* ¶ 14; *cf. United States v. Olson*, 856 F.3d 1216, 1220 (9th Cir. 2017) ("[Courts] ordinarily read a phrase in

a criminal statute that introduces the elements of a crime with the word 'knowingly' as applying that word to each element" (citation omitted)). Thus, Plaintiffs do not, and cannot, plead that Renaissance ***knew*** it lacked permission to receive and process students' data.

***Second***, CDAFA defines "[a]ccess" to mean "to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1). "While [CDAFA] has been extended by some district courts outside of the traditional hacking realm," courts still require a showing that "defendant in some way caused output from the function of a computer, without the owner's permission." *Heiting*, 709 F. Supp. 3d at 1020. Plaintiffs do not allege that Renaissance collected data from or accessed parts of their children's computers ***outside*** of Renaissance's products. *See id*. (dismissing CDAFA claim where defendant's alleged collection of data did not satisfy "access" element because plaintiff did not allege "that [d]efendant implanted anything on her computer" or otherwise "make clear how any 'access' took place").

Thus, Plaintiffs' CDAFA claim should be dismissed.

### D. Plaintiffs' UCL Claim Fails Because They Lack Standing and Do Not Plausibly Plead Any of the Prongs (Count V).

Plaintiffs' UCL claim similarly fails for both lack of statutory standing and failure to allege the requisite elements.

No statutory standing. To have UCL standing, plaintiffs must plead that they "lost money or property as a result of the unfair competition." *Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009). Plaintiffs allege that they suffered loss based on Renaissance's alleged "unauthorized disclosure and taking of [their children's] personal information" and the resulting "diminution of the value of their private and personally identifiable data and content." FAC ¶ 428. Neither theory is viable.

As to Plaintiffs' "unauthorized taking" theory, "[n]umerous courts have held

that disclosure of personal information alone does not constitute economic or property loss sufficient to establish UCL standing[.]" *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1144 (E.D. Cal. 2021); *see Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928, 943 (N.D. Cal. 2023) ("[t]he weight of the authority . . . [holds] that the mere misappropriation of personal information does not establish compensable damages" under the UCL (citation modified)); *Cappello v. Walmart Inc.*, No. 18-cv-06678-RS, 2019 WL 11687705, at *4 (N.D. Cal. Apr. 5, 2019) ("[p]laintiffs must allege more than a loss of personal information to establish standing under the UCL.").

Plaintiffs' "diminution of value" theory fares no better because they fail to plausibly "allege they ever attempted or intended to participate in [the] market [for their PII], or otherwise to derive economic value from their PII." *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538–39 (2022). Courts have dismissed UCL claims in edtech data privacy matters predicated on the "diminution of value" framework, because "there is no nonspeculative basis . . . for thinking plaintiffs can or would transact with the personal information at issue, such as their exam scores or behavioral assessments . . . [In fact,] [i]t is reasonable to infer that plaintiffs would choose *not* to transact in that market" given their alleged privacy interests in such data. *Cherkin v. PowerSchool Holdings, Inc.*, No. 24-cv-02706-JD, 2025 WL 844378, at *5 (N.D. Cal. Mar. 17, 2025); *see Instructure*, 2025 WL 2233210, at *6 (dismissing UCL claim in edtech case because "allegations about the loss of value of data" did not confer statutory standing).

To evade this threshold standing requirement, Plaintiffs add unsupported allegations that Renaissance "prevented the development of a legitimate market for student data" and that "Plaintiffs would consider participating in a market for their information" under hypothetical conditions. FAC ¶ 430. Given that Plaintiffs elsewhere plead that the information allegedly collected by Renaissance is "highly personal and sensitive," *id.* ¶¶ 73, 441, this attempt to "self-engineer" statutory

standing is unavailing. In any event, Plaintiffs' imagining a theoretical market in which they might participate is insufficient to confer UCL standing, which requires that Plaintiffs "attempt[] or intend[] to participate" in an ***existing*** market. *See Moore*, 83 Cal. App. 5th at 538–39.

No claim under any UCL prong. Plaintiffs' unlawful prong theory is premised "state and federal law" violations pled elsewhere in the FAC. FAC ¶ 427. Because Plaintiffs' statutory claims are deficient, their derivative UCL claim also fails. *See Aleksick v. 7-Eleven, Inc.*, 205 Cal. App. 4th 1176, 1185 (2012) ("When a statutory claim fails, a derivative UCL claim also fails."). Plaintiffs' common law claims, meanwhile, cannot form the basis of an unlawful prong claim. *See Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1043–44 (9th Cir. 2010) (common law violations are insufficient for UCL unlawful prong claims).

Similarly, Plaintiffs' unfair prong claim fails because it is based on the same alleged conduct as their meritless claims under the other prong(s). *See Hadley v. Kellogg Sales Co.*, 243 F. Supp. 3d 1074, 1104–05 (N.D. Cal. 2017) (where the unfair prong "overlap[s] entirely with . . . the fraudulent and unlawful prongs of the UCL, the unfair prong of the UCL cannot survive if the claims under the other two prongs of the UCL do not survive").[8]

[8] The FAC does not explicitly invoke the UCL's fraudulent prong. FAC ¶¶ 419–432. Even had Plaintiffs attempted to do so, their claim would fail because they do not plead that they were exposed to any of Renaissance's alleged misrepresentations prior to their children using Renaissance's products, let alone plead with Rule 9(b) particularity that they relied on those misrepresentations to their detriment. *See Figy v. Amy's Kitchen, Inc.*, No. CV 13–03816 SI, 2013 WL 6169503, at *4 (N.D. Cal. Nov. 25, 2013) (collecting cases); *see also Sateriale v. R.J. Reynolds Tobacco Co.*, 697 F.3d 777, 793 (9th Cir. 2012) ("actual reliance on the allegedly deceptive or misleading statements," along with causation, required to state a fraud-based UCL claim).

**E. Plaintiffs' Intrusion Upon Seclusion Claim Fails as They Do Not Allege a Physical Intrusion or Demonstrate That They Provided Data to Renaissance Unwillingly (Count VI).**

In Wisconsin, the tort of intrusion upon seclusion penalizes an "[i]ntrusion upon the privacy of another of a nature highly offensive to a reasonable person . . . in a ***place*** that a reasonable person would consider private or in a manner that is actionable for trespass." Wis. Stat. Ann. § 995.50(2)(am) (emphasis added).

Courts consistently hold that the word "place" in the statute is "geographical," requiring an actual physical incursion—it does not cover alleged violations of an individual's "private affairs or concerns[.]" *See Hillman v. Columbia Cnty.*, 474 N.W.2d 913, 919 (Wis. Ct. App. 1991); *see also Buckeridge v. Univ. of WI Hosp. & Clinics Auth. UW Health*, 932 N.W.2d 185, 185 (Wis. Ct. App. 2019) (dismissing an intrusion claim predicated on defendant's alleged wrongful disclosure of plaintiff's health information to third parties because "records stored on . . .[a] computer system are [not] 'geographical'"); *see also Doe v. Saftig*, No. 09-C-1176, 2011 WL 1792967, at *14 (E.D. Wis. May 11, 2011) (dismissing an intrusion claim predicated on defendant's alleged wrongful disclosure of plaintiff's personal information to third parties, as it "does not involve an intrusion into a private 'place'… or private 'belongings'").

Here, Plaintiffs' intrusion claim is predicated solely on Renaissance's alleged misuse and wrongful disclosure of personal information collected from students accessing Renaissance's digital platforms. *See* FAC ¶¶ 435–36. Such conduct does not constitute a violation of any geographical or physical "space" and therefore cannot be the subject of an intrusion claim under Wisconsin law. [9]

[9] Even if an intrusion into an electronic device were actionable, Plaintiffs and their children had no cognizable privacy interest in the "school-issued" devices that their children allegedly used to access Renaissance platforms. FAC ¶¶ 25–29. *See In re Isiah B.*, 500 N.W.2d 637, 641 (Wis. 1993) (students have no reasonable expectation of privacy over school property temporarily leased to them). The intrusion claim also fails because the information at issue was provided "willingly." FAC ¶¶ 50–51, 61–

### F. Plaintiffs' Theory of Liability Fails to Establish Unjust Enrichment Under Wisconsin Law (Count VII)[10]

Plaintiffs have not stated an unjust enrichment claim because students' "confer[ral]" of personal information to Renaissance does not constitute the required tangible benefit. *See* FAC ¶ 449. Indeed, the only decision Renaissance located applying Wisconsin law to the "question of whether the conferral of PII can itself constitute a benefit for purposes of unjust enrichment" held that it could not. *See Giasson v. MRA - Mgmt. Ass'n, Inc.*, 777 F. Supp. 3d 913, 940-41 (E.D. Wis. 2025) (noting caselaw trend of "reject[ing] unjust enrichment claims premised on this theory"; dismissing PII-related unjust enrichment claim where complaint "lack[ed] any contextualizing information as to what role Plaintiff's PII played in Defendant's business operation and how Defendant's retention of her PII benefitted Defendant in some measurable, economic sense").

The FAC does not allege that Renaissance received any other tangible benefit. It at most speculates that Renaissance obtained investors because it collects student data. *See* FAC ¶ 47. And Plaintiffs rely on vague assertions about the market for "user data," *see id.* ¶ 307, but do not allege what value (if any) the alleged collection and use of student data offers to Renaissance's business, let alone what value Plaintiffs' children's data specifically would have.

Further, "under Wisconsin's law of unjust enrichment[,] it is not inequitable for one to benefit from the willful disclosure of information or an idea when such an idea . . . is not protected by some sort of intellectual property right." *Fail Safe LLC v. A.O. Smith Corp.*, 762 F. Supp. 2d 1126, 1130 (E.D. Wis. 2011), *aff'd,* 674 F.3d 889 (7th Cir. 2012); *see ConFold Pac., Inc. v. Polaris Indus., Inc.*, 433 F.3d 952, 957 (7th Cir. 2006) ("Wisconsin law denies recovery for unjust enrichment if all the

---

62, 77–78; *Linman v. Marten Transp., Ltd.*, No. 22-CV-204-JDP, 2023 WL 2562712, at *6 (W.D. Wis. Mar. 17, 2023).

[10] Plaintiffs bring Count VII "pursuant to Wisconsin Law." FAC at p. 79.

defendant has done is use (to his profit) an idea of the plaintiff that is not a trade secret."). Plaintiffs do not allege any intellectual property or trade secret rights in any information they knowingly inputted into a Renaissance platform. Thus, even were Plaintiffs correct that Renaissance uses this information solely for its own profit (they are not), they would not have stated an unjust enrichment claim.

Finally, "[u]njust enrichment involves getting something for nothing, not providing a product for a price." *T&M Farms v. CNH Indus. Am., LLC*, 488 F. Supp. 3d 756, 769 (E.D. Wis. 2020). Where a party "receive[s] something in return for the benefit they supposedly conferred" but finds the return service "did not meet expectations," they are entitled to pursue legal remedies but cannot obtain equitable relief based on an unjust enrichment theory. *Id.* Here, Plaintiffs allege that Renaissance provided their children with access to its educational platforms and products in exchange for a wrongful conferral of users' personal information. In short, Plaintiffs admittedly received a benefit from their use of Renaissance's products (*see* FAC ¶¶ 50–51, 57, 61–62, 68–70, 77–78), requiring dismissal of their unjust enrichment claim.

**G. Plaintiffs Fail to Plead a Plausible Negligence Claim (Count VIII)**

Plaintiffs fail to state a negligence claim either under a classic or negligence *per se* theory of liability.

***First***, while Wisconsin "follows the minority view that everyone owes to the world at large the duty of refraining from those acts that may unreasonably threaten the safety of others," plaintiffs must still allege a "foreseeable" breach of the defendant's duty. *Mitchell v. Hess*, No. 08-C-847, 2010 WL 1212080, at *3 (E.D. Wis. Mar. 23, 2010) (internal quotations and citations omitted). As discussed, Renaissance—like numerous other edtech companies—has long followed FTC guidance that expressly permits them to enter the service arrangements with schools and school districts at issue here. When Renaissance contracted with Plaintiffs' children's schools, it was not foreseeable that Plaintiffs would later claim that these

common arrangements constituted a privacy violation (let alone that such claims could have any merit). Permitting this claim would thwart the edtech industry's ability to provide services key to students' educational experiences—an unfavorable outcome that counsels against an imposition of liability. *See Pelnar v. Rosen Sys., Inc.*, 964 F. Supp. 1277, 1284 (E.D. Wis. 1997) (ruling for defendant on negligence claim where "public policy dictate[d] a limitation of liability" because imposing liability "would open up the possibility that no sensible or just stopping point exists").

Additionally, "Wisconsin courts haven't hesitated to preclude [negligence] liability when . . . there was an intervening cause with a more direct causal relationship to the harm." *Dawson v. Great Lakes Educ. Loan Servs., Inc.*, No. 15-CV-475-JDP, 2022 WL 1500447, at *6 n. 4 (W.D. Wis. May 12, 2022) (collecting cases), *aff'd,* No. 22-2189, 2025 WL 800237 (7th Cir. Mar. 13, 2025); *see Spierer v. Rossman*, 798 F.3d 502, 510 (7th Cir. 2015) (noting that a "criminal act [by a third party] . . . breaks the causal chain between the alleged negligence and the resulting harm."). Plaintiffs' negligence claim is based at least partially on speculation that third parties ***might*** misuse data received from Renaissance. FAC ¶¶ 468, 474. However, Renaissance can lawfully make certain disclosures of student data to third parties, such as to "allow or improve operability and functionality[.]" *See* Cal. Bus. & Prof. Code § 22584(b)(4); *see* Section II.A. If any third parties subsequently misused the disclosed data, their (hypothetical) unlawful conduct would sever any causal link between Renaissance's supposed negligence and the alleged damages to Plaintiffs.

Finally, Plaintiffs must plead "actual damages." *Lemmermann v. Blue Cross Blue Shield of Wis.*, 713 F. Supp. 2d 791, 811 (E.D. Wis. 2010). Plaintiffs assert the "diminution in value of their intimate personal information." FAC ¶ 484. As discussed *supra*, Section IV.D, this theory is nonviable given Plaintiffs' own disinterest in participating in any currently existing market for internet users' data. Moreover, Plaintiffs fail to explain what actual damages have resulted from "the

improper collection, exposure, [and] exploitation" of their personal information. FAC ¶ 484.

***Second***, Plaintiffs' attempt to plead a negligence *per se* claim based on Renaissance's alleged COPPA violations, *id.* ¶ 477, is nonviable because that theory only applies under Wisconsin law to claims based on the defendant's violation of a "safety statute"—which does not exist here.[11] Specifically, a *per se* instruction is available only in "a narrowly defined range of circumstances." *Cooper v. Eagle River Mem'l Hosp., Inc.*, 270 F.3d 456, 460 (7th Cir. 2001). "In distinguishing 'safety statutes' from more general regulatory measures, ***plaintiffs must do more than baldly assert that the statute in question protects a specific class of individuals***. All legislation promotes the public welfare to some degree. Instead, the legislation must evince a clear and unambiguous legislative desire to establish civil liability." *Id.* (emphasis added). Wisconsin courts have held that even laws regulating the licensure of medical professionals do not qualify as "safety statutes" when there is no evidence of "legislative intent to grant a private right of action for a violation of the statute." *Leahy by Heft v. Kenosha Mem'l Hosp.*, 348 N.W.2d 607, 612 (Wis. Ct. App. 1984).

As Plaintiffs themselves note, "COPPA does not contain an express private right of action." FAC ¶ 473. Given that Congress has not authorized its private enforcement, COPPA would be deemed a "general regulatory measure," rather than a "safety statute[.]" This means Plaintiffs do not (and cannot) state a negligence claim based on Renaissance's alleged failure to comply with COPPA.

[11] A safety statute is a "legislative enactment designed to protect a specified class of persons from a particular type of harm." *Totsky v. Riteway Bus Serv., Inc.*, 607 N.W. 2d 637, 648–44 (Wis. 2000) (citation omitted) ("stop sign statute[, requiring vehicles to stop at stop signs,] is a safety statute, the violation of which constitutes negligence per se); *see also Johnson v. Blackburn*, 582 N.W.2d 488, 498 (Wis. Ct. App. 1998) (statute requiring installation of smoke detectors is a safety statute).

**H. Plaintiffs' WDTPA Claim Should Be Dismissed (Count X)**

Plaintiffs' Wisconsin Deceptive Trade Practices Act ("WDTPA") claim fails for several reasons.

***First***, Plaintiffs cannot pursue a WDTPA claim because they and their children were "[a]t all relevant times" citizens and residents of California (FAC ¶¶ 25–26) and Kansas (*id.* ¶¶ 28–29), respectively, when they were exposed to Renaissance's alleged misconduct—but the WDTPA "affords a remedy ***only*** to Wisconsin consumers[.]" *See Hydraulics Int'l, Inc. v. Amalga Composites, Inc.*, No. 20-CV-371, 2022 WL 4273475, at *10 (E.D. Wis. Sep. 15, 2022) (emphasis added); *accord id.* at *9 ("The only reasonable reading of the statute is that it applies only to Wisconsin consumers.").

***Second***, the WDTPA prohibits parties from undertaking "untrue, deceptive, or misleading" conduct with the intent to "sell, distribute, increase the consumption of or in any [way] dispose of any real estate, merchandise, securities, employment, service, or anything offered by such person[.]" Wis. Stat. § 100.18(1). Per its plain language, the WDTPA applies only to "commercial transactions." *Slane v. Emoto*, 582 F. Supp. 2d 1067, 1083 (W.D. Wis. 2008); *see also Thermal Design, Inc. v. Am. Soc'y of Heating, Refrigerating & Air-Conditioning Eng'rs, Inc.*, 755 F.3d 832, 837 (7th Cir. 2014) (noting that the WDPTA applies only to alleged misrepresentations made to "promote the sale of a product" (emphasis omitted; citation omitted)). Plaintiffs do not allege entering any commercial transaction with Renaissance, requiring dismissal.

***Third***, Plaintiffs fail to allege a "pecuniary loss," which requires "a causal connection" between Renaissance's statements and any alleged pecuniary loss Plaintiffs experienced. *Dusterhoft v. OneTouchPoint Corp.*, No. 22-cv-0882-BHL, 2024 WL 4263762, at *16 (E.D. Wis. Sept. 23, 2024). The FAC vaguely alleges that Renaissance's alleged misrepresentations were made to "Plaintiffs…***and/or*** their schools." FAC ¶ 512 (emphasis added). However, Plaintiffs do not plausibly allege

that their children or they were "materially induced" to transact with Renaissance by the challenged statements. *Weaver v. Champion Petfoods USA Inc.*, 3 F.4th 927, 934 (7th Cir. 2021) (noting that a WDTPA claim requires a showing of harm "***to the plaintiff***") (emphasis added) (citation omitted). And even if Plaintiffs could demonstrate the requisite causal connection, for the reasons discussed *supra*, Section IV.D, Plaintiffs and their children have not suffered tangible economic injury from Renaissance's alleged conduct.

## V. CONCLUSION

For these reasons, the FAC should be dismissed in full. As Plaintiffs already amended once but failed to cure the many legal deficiencies identified previously, the Court should dismiss the FAC with prejudice, particularly as the fundamental theory underlying Plaintiffs' complaint disregards an established regulatory regime specific to the school setting. *See, e.g., Hadley*, 243 F. Supp. 3d at 1089 n.1 (N.D. Cal. 2017) (dismissing with prejudice where "FAC failed to cure th[e] deficiency identified in [d]efendant's motion to dismiss the original complaint.").

Dated: October 30, 2025

COOLEY LLP

By: */s/ Matthew D. Brown*
Matthew D. Brown

Attorneys for Defendant
RENAISSANCE LEARNING, INC.